

**Information Security Office - Security Incident Tracking Log**  
**Third Quarter FYE 06-30-11 (11-23-10 to 02-24-11)**

**Attachment 1**

<b>Incident Number</b>	<b>Type of Incident</b>	<b>Official Notification Date of Incident Sent to ISOF</b>	<b>Originating Division, Branch, or Office</b>	<b>Comments</b>
11-13 (IN)	Missing BlackBerry 9700 Bold Smartphone	11/30/10	FCSD	Based on the investigative work performed to date (12-01-10), the ISOF infers on the basis of the evidence collected and examined that a CalPERS employee first noted his CalPERS assigned BlackBerry Bold 9700 smartphone handheld device was missing on November 28, 2010 at his personal residence. The employee states that no sensitive data was stored on the smartphone. The device was password protected and a command was issued to wipe all data from the device.
11-14 (IN)	Lost RSA Token	12/06/10	ITSB	Based on the investigative work performed to date (12-07-10), the ISOF infers on the basis of the evidence collected and examined that a CalPERS employee misplaced her assigned RSA token card at her home residence, during the weekend of December 4, 2010 and December 5, 2010. The misplaced token was disabled and noted as lost. A new token was issued.
11-15 (IN)	Lost RSA Token	12/06/10	MBSB	Based on the investigative work performed to date (12-07-10), the ISOF infers on the basis of the evidence collected and examined that a CalPERS employee misplaced his assigned RSA token card. The misplaced token was disabled and noted as lost. A new token was issued.
11-16 (IN)	Unauthorized Disclosure of SSN	12/15/10	CSFD	Based on the investigative work performed to date (12/29/10), the ISOF infers on the basis of the evidence collected and examined that the Social Security number for Member A was disclosed to Member B in an unauthorized manner. A Service Retirement application and rejection letter for Member A was mailed to Member B. Member B reported the incident to CalPERS. An employee in the mailroom accidentally sorted and manually stuffed two members' documents into one envelope. The manager was reminded that a second person is to check the first persons work in order to alleviate this the of error. A Privacy Breach Notification letter is not necessary pursuant to California Civil Code Section 1798.29. In addition, a letter offering CSIdentity Theft Insurance was mailed to Member A.

**Information Security Office - Security Incident Tracking Log**  
**Third Quarter FYE 06-30-11 (11-23-10 to 02-24-11)**

**Attachment 1**

Incident Number	Type of Incident	Official Notification Date of Incident Sent to ISOF	Originating Division, Branch, or Office	Comments
11-17 (IN)	State Employee Impersonating a CalPERS Representative	12/23/10	CSED	<p>Based on the investigative work performed to date (12/30/10), the ISOF infers on the basis of the evidence collected and examined that an employee of another agency misrepresented themselves as a CalPERS employee and made harmful statements to a California Highway Patrol Officer, abusing their position as a State of California employee.</p> <p>Since this employee is with another agency, this incident has been formally transferred to that agency's Information Security Officer.</p>
11-18 (IN)	Unauthorized Disclosure of SSNs	12/23/10	BNSD	<p>Based on the investigative work performed to date (01/19/11), the ISOF infers on the basis of the evidence collected and examined that the SSN number for Member C's beneficiary and Member D's beneficiary were accidentally entered by the Retirement Benefit Processing and Maintenance staff in the data field reserved for the city the member lives in. This was reported by the Document Management Center who identified a social security number in the address of the BAS-11 being mailed to Member C and D and escalated this incident. Although the BAS -11 never left the building a Service Retirement Congratulation Letter was also automatically generated and was sent to Member C and Member D with their beneficiary's SSN displayed in the address window of the mailing envelope resulting in a security breach.</p> <p>The CalPERS employee who made the error has received remedial training on how to avoid this error in the future. The Benefit Services Division, Retirement Calculation and Adjustment Section has contacted the Automation Support Section to request a system audit for both the Retirement Information and Benefit System and Retirement Application Process System to ensure the screen audits for both systems will not allow anything that looks like a SSN to be entered and saved in the address field. A privacy Breach Notification letter is not necessary pursuant to California Civil Code Section 1798.29. Member C and Member D's beneficiary's were offered CSIdentity Theft Insurance.</p>

**Information Security Office - Security Incident Tracking Log**  
**Third Quarter FYE 06-30-11 (11-23-10 to 02-24-11)**

**Attachment 1**

<b>Incident Number</b>	<b>Type of Incident</b>	<b>Official Notification Date of Incident Sent to ISOF</b>	<b>Originating Division, Branch, or Office</b>	<b>Comments</b>
11-19 (IN)	Harmful Statements Made to a CHP Officer	12/28/10	HRSD	<p>Based on the investigative work performed to date (02/10/2011), the ISOF infers on the basis of the evidence collected and examined that a CalPERS employee made harmful statements to two California Highway Patrol Officers.</p> <p>CHP Special Investigation Unit conducted a follow up investigation, and determined that the employee's comments were not sincere and would not be acted upon. They requested that no further action be taken.</p> <p>HRSD has pursued personnel action against the employee for abusing their position as a State of California employee.</p>
11-20 (IN)	Items from Confidential Destruct Bin Blown onto 3rd Street	12/29/10	ITSD	<p>Based on the investigative work performed to date (01/04/11), the ISOF infers on the basis of the evidence collected and examined that confidential documents were released in an unauthorized manner during the onsite shredding of confidential documents. In this instance a container of confidential documents fell over on a very windy day and began to blow across the street into the adjacent parking lot. The ISOF was contacted immediately and supervised the retrieval of the documents. All papers were retrieved based on staff assisting with the collection and verified by staff observing from the 3<sup>rd</sup> floor of LPW, facing 3<sup>rd</sup> Street. Corrective action has been taken to prevent a reoccurrence of this incident. Documents will be loaded from the locked bins into the shredder inside the loading dock and not on the street.</p>
11-21 (IN)	Missing BlackBerry 9700 Bold Smartphone	01/04/11	ITSD/PSR	<p>Based on the investigative work performed to date (01-11-11), the ISOF infers on the basis of the evidence collected and examined that CalPERS employee first noted her CalPERS assigned BlackBerry Bold 9700 smartphone handheld device was missing on December 28, 2010. She states that no sensitive data was stored on the smartphone. The device was password protected and a command was issued to wipe all data from the device.</p>

**Information Security Office - Security Incident Tracking Log**  
**Third Quarter FYE 06-30-11 (11-23-10 to 02-24-11)**

**Attachment 1**

Incident Number	Type of Incident	Official Notification Date of Incident Sent to ISOF	Originating Division, Branch, or Office	Comments
11-23 (IN)	Unauthorized Disclosure of SSN and Financial Acct. Number	02/09/11	BNSD	Based on the investigative work performed to date (02-15-11), the ISOF infers on the basis of the evidence collected and examined that the Social Security number and financial account number for Member E was disclosed to Member F in an unauthorized manner. These two members had the same first and last name but a different middle initial. In this incident a retirement benefit for Member E was deposited incorrectly into Member F's bank account. In addition, a 2010IRS Form for Member E was also mailed to Member F's home address by mistake. CalPERS was notified of the incident by Member F. The error was a result of the BNSD Forms and Roll Unit changing the SSN on Member E's documents to that of Member F. The Benefit Specialist processing the documents assumed the new SSN was correct and proceeded to approve the payment. The Specialist has subsequently been retrained on the importance of verifying the full name, address and SSN and not assuming the correction made by key entry is accurate. A <i>Privacy Breach Notification</i> letter is necessary pursuant to California Civil Code Section 1798.29. A letter offering <i>CSIdentity Theft Insurance</i> was mailed to Member E.
11-24 (IN)	Unauthorized Disclosure of SSN	02/15/11	MBSD	Based on the investigative work performed to date (02-23-11), the ISOF infers on the basis of the evidence collected and examined that the Social Security number for Member G was disclosed to Member H in an unauthorized manner. An Additional Retirement Service Credit (ARSC) costing package for Member G was accidentally mailed to Member H along with Member H's ARSC. Member H notified CalPERS and has shredded the information received in error. The employee who made the mistake has been counseled and the personnel issue has been elevated. The employee has received remedial training on the Division procedures. All Quality Control Checkers were reminded of the importance of checking outgoing mail. A <i>Privacy Breach Notification</i> letter is not necessary pursuant to California Civil Code Section 1798.29. However, a letter offering <i>CSIdentity Theft Insurance</i> was mailed to Member G.

**Information Security Office - Security Incident Tracking Log**  
**Third Quarter FYE 06-30-11 (11-23-10 to 02-24-11)**

**Attachment 1**

Incident Number	Type of Incident	Official Notification Date of Incident Sent to ISOF	Originating Division, Branch, or Office	Comments
11-26 (IN)	Lost Thumb Drive	02/18/11	BNSD	Based on the investigative work performed to date (02-23-11), the ISOF infers on the basis of the evidence collected and examined that a thumb drive assigned to a CalPERS employee is missing. The business activities and interim procedures do not contain any confidential information or personally identifiable information. In addition, the thumb drive was password protected. No further action is required.